ROUTING DRIVEN PROTOCOL FOR SECURE DATA TRANSFER SATISFYING QOS CONSTRAINTS

S. Ravichandran,[1]
Associate Professor,
Department of Information Technology,
Sri Krishna Engineering College
Mail-id: ravi17raja@gmail.com
Dr.E.R. Naganathan,[2]
Professor & Head,
Department of Computer Science & Engineering,
Hindustan University
Mail-id: ernindia@gmail.com

ABSTRACT-
Due to the fact that the wireless links in an Adhoc network are susceptible to attacks and the nodal mobility renders the network to have a highly dynamic topology, it becomes critical to detect major attacks against the routing protocols of such networks and also provide some extent of QoS to the network traffic. In this paper, going to present a new secure routing protocol (SRP) with quality of service (QoS) support, called Trustworthiness-based Quality Of Service (TQOS) routing, which includes secure route discovery, secure route setup, and trustworthiness-based QoS routing metrics. The routing control messages are secured by using both public and shared keys, which can be generated on-demand and maintained dynamically. The message exchanging mechanism also provides a way to detect attacks against routing protocols, particularly the most difficult internal attacks. The routing metrics are obtained by combing the requirements on the trustworthiness of the nodes in the network and the QoS of the links along a route. The simulation results have demonstrated the effectiveness of the proposed secure QoS routing protocol in both security and performance and also the paper is to be extend using the cryptography technique called Elliptic Curve Cryptography and also performs secure data transfer using Adhoc networks. Enhancing it in suitable battle field communication and also to look into quality of service .These all need to be further investigated.

Key Words- **Security, QoS, Routing Protocol, Adhoc networks.**

1.0 INTRODUCTION

The Network in Wireless Adhoc started to be deployed in different environment. A very particular challenging problem is that how to detect the major attack against the routing protocol in its design where some Qos supports to the network traffic. First of all the routing protocol has to defend the attack which may come from internal or external node in a secured manner. In an external attack, a malicious node masquerades as a trusted node although it does not participate in the routing process. It can get floods of inauthentic service request, such as Denial of service attack. While in an Internal attack there may be a possibility of the node being like compromised or misconfigured node participating routing, or even colludes with other malicious nodes, which is called a Byzantine attack . It may advertise false routing information, not forward packet correctly, misroute, fabricate, modify, or simply drop packets. Therefore, it is more difficult to detect the internal attacks. Second, the protocols must be integrated with QoS routing schemes to support the QoS requirements of the carried traffic, for example, to minimize a cost under delay constraint, or minmax a cost caused by a single link failure or by co- channel interferences. The existing SRPs for ad hoc networks often avoid either the most challenging internal attacks, such as Byzantine behaviours, or the QoS requirements of the traffic.

The fact that security is a critical problem when implementing MANETs is widely acknowledged. One of the different kinds of misbehaviour a node may exhibit is selfishness. A selfish node wants to preserve own resources. One way of preventing selfishness in a MANET is a detection and exclusion mechanism. This project focuses on the detection phase and present different kinds of techniques that can be used to find selfish nodes. The detection mechanisms described are called activity-based overhearing, iterative probing, and unambiguous probing.

1.1 PROBLEM DEFINITION

In wireless networks, signals are transmitted via open

and shared media. Without protection, anyone in the transmission range of the sender can intercept the sender's signal. Therefore, wireless communications are inherently less secure than their wired counterparts. Furthermore, wireless devices usually have limited bandwidth, storage space, and processing capacities. It is harder to reinforce security in wireless networks than in wired networks.

Compared with WLANs, the security management in wireless ad hoc networks is much tougher due to the following characteristics.

1.1.1 Resource Constraints: The wireless devices usually have limited bandwidth, memory and processing power . This means costly security solutions may not be affordable in wireless ad hoc networks.

1.1.2 Unreliable Communications: The shared-medium nature and unstable channel quality of wireless links may result in high packet-loss rate and re-routing instability, which is a common phenomenon that leads to throughput drops in multi-hop networks. This implies that the security solution in wireless ad hoc networks cannot rely on reliable communication.

1.1.3 Node mobility and dynamic topology: The network topology of wireless Adhoc network may change rapidly and unpredictably over time, since the connectivity among the nodes may vary with time due to node departures, node arrivals, and the mobility of nodes. This emphasizes the need for secure solutions to be adaptive to dynamic topology.

1.1.4 Scalability: Due to the limited memory and processing power on mobile devices, the scalability is a key problem when to consider a large network size. Networks of 10,000 or even 100,000 nodes are envisioned, and scalability is one of the major design concerns.

1.2 OBJECTIVE

To enhance the AODV protocol by incorporating security features into it. AODV is basically a protocol designed for efficient routing. Security features are to be added to it to make it a SRP. A major enhancement to it includes identification of the malicious node. A malicious node is a privileged node that indulges in internal attacks. Other enhancements include the incorporation of link to link authentication. Route Discovery and Route maintenance, which is an integral part of all secure routing protocols, is also considered.

1.3 LITERATURE SURVEY

The existing SRPs for ad hoc networks can be divided into two categories: in terms of how an SRP is secured and what types of attacks it can defend. In the first category, the commonly used method is to establish a security association between the source and destination nodes so that the on-demand routing protocols, such as AODV, DSR, and DSDV, can be secured. There is an SRP called Ariadne based on DSR that uses efficient symmetric cryptography. Routing messages are authenticated by shared secrets between each pair of nodes. The broadcast authentication scheme used in Ariadne is TESLA, which requires loose time synchronization. In, the authors proposed a proactive SRP, called SEAD, based on DSDV by using one-way hash chains to provide authentication to defend attacks that modify routing information broadcast and replay attacks but not wormhole attack. In order to secure on-demand protocols such as AODV and DSR, the authors developed an authenticated routing protocol, called ARAN, by using digital signature to provide end-to-end authentication, message integrity, and non repudiation. During route discovery, a routing message is signed by a source node and then broadcasted to others. An intermediate node that receives the message will replace the certificate and signature of the previous hop with those of its own and then forwards the message to the next hop. During route setup, the message is similarly signed twice and unicasted back to the source. Due to its use of double signatures, ARAN can defend most common attacks.

In the second category, the major purpose is to protect routing traffic against the internal attacks, particularly Byzantine attacks. Some authors proposed to use both route and message redundancy to detect Byzantine behaviours by comparing different copies of a message received over different routes. In a research, the authors proposed to detect Byzantine behaviours by using a probing technique, which uses binary search on a path to find out faulty links. The accumulated path is protected by an aggregate signature scheme, which is even more expensive than RSA signatures. Few authors have proposed an SRP against Byzantine failures by using source routing and destination acknowledgements. Each packet is authenticated at each node by using MACs based on pair-wise secret keys. Misbehaviours are detected on a per packet basis to defend Byzantine adversaries.

2.0 ADHOC NETWORK

A mobile ad hoc network is a network formed and

functioning without any established infrastructure or centralized administration and consists of mobile nodes that use a wireless interface to communicate with each other. These mobile nodes serve as both hosts and routers so they can forward packets on behalf of each other. Hence, the mobile nodes are able to communicate beyond their transmission range by supporting multihop communication.

The benefits of ad hoc networks are quick installation due to absence of wire line infrastructure, mobility, since nodes can communicate while in motion and natural capabilities of reconfiguration and redeployment. These advantages make ANETs ideal for many applications, from personal area networks to large sensor networks. However, the native properties of radio transmission and frequent topology changes due to node mobility create many challenging research problems. Mobile ad hoc networks share many of the properties of wired-infrastructure LANs but also possess certain unique features which derive from the nature of the wireless medium and the distributed function of the medium access mechanism. Such constraints are wireless channel, the mobile node and the routing protocol which are used to establish and maintain communication paths. These characteristics affect the functionality of mechanisms throughout the communication protocol stack. Ad hoc network hosts can use protocols such as the IEEE 802.11 media-access control standard to communicate via the same frequency or they can apply Bluetooth or other frequency-hopping technology.

2.1 EXISITING MANET SECURITY PROTOCOL

Based on the existing protocols, an effort has been made to chalk out strategy adopted by each protocol, its merits and demerits.

2.1.1 SRP: It's the protocol which assumes security association between source destination nodes. The Intermediate nodes do not need cryptography Adds a SRP header to base routing protocol, It has three parts taking care of old outdated request, prevents fabrication and ensures integrity.

2.1.2 ARAN: Assume managed-open environment which has the First stage is certification and end-to-end authentication stage each intermediate node signs the request with its certification

2.1.3 ARIADNE: Uses highly efficient symmetric key cryptography with No guard against passive attackers and also does not prevent insertion of malicious data packets. Vulnerable to other attackers form broken link

2.1.4 SEAD: Uses one way hash function. Attacker cannot generate any value in hash chain. Very efficient Mechanism.

2.1.5 SAODV: Implementation on AODV which Checks for external attacks. Uses Key cryptography and hashing both.

2.1.6 SAR: Classifies nodes into different and Immutable trust levels. Can be implemented by distributing Keys for each trust level. Not very scalable. Lot of computational efforts required.

2.2 RELATED WORK

The existing SRPs for ad hoc networks can be divided into two categories: in terms of how an SRP is secured and what types of attacks it can defend. In the first category, the commonly used method is to establish a security association between the source and destination nodes so that the on-demand routing protocols, such as AODV, DSR, and DSDV, can be secured. There is an SRP called Ariadne based on DSR that uses efficient symmetric cryptography. Routing messages are authenticated by shared secrets between each pair of nodes. The broadcast authentication scheme used in Ariadne is TESLA, which requires loose time synchronization. In, the authors proposed a proactive SRP, called SEAD, based on DSDV by using one-way hash chains to provide authentication to defend attacks that modify routing information broadcast and replay attacks but not wormhole attack. In order to secure on-demand protocols such as AODV and DSR, the authors developed an authenticated routing protocol, called ARAN, by using digital signature to provide end-to-end authentication, message integrity. During route discovery, a routing message is signed by a source node and then broadcasted to others.. During route setup, the message is similarly signed twice and unicasted back to the source. Due to its use of double signatures, ARAN can defend most common attacks.

In the second category, the major purpose is to protect routing traffic against the internal attacks, particularly Byzantine attacks. Some authors proposed to use both route and message redundancy to detect Byzantine behaviors by comparing different copies of a message received over different routes. In a research, the authors proposed to detect Byzantine behaviors by using a proprobing technique, which uses binary search on a path to find out faulty links.

2.3 OBSERVANCE FROM LITERATURE SURVEY

Based on the above review, to conclude that few protocols are capable of detecting internal attacks such as Byzantine attacks and use expensive aggregate signatures or per packet filtering. Also, the routing metrics are still performance indicators, not security metrics, such as the trustworthiness of a node. Therefore, few routing protocols consider the security and QoS problems together. Specifically the energy of a node is not considered.

3.0 PROPOSED WORK

MANETs rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer track, the more powerful a MANET gets. But supporting a MANET is a cost-intensive activity for a mobile node. Detecting routes and forwarding packets consumes local CPU time, memory,

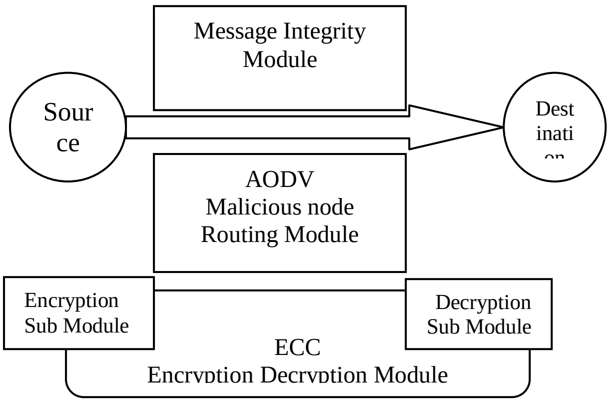

Fig. 1 Architecture of the Proposed System

Network-bandwidth and last but not least energy. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data.

The message exchange mechanism also provides a way to detect against routing protocols, particularly the most difficult internal attacks. The routing metrics are obtained by combining the requirements on the trustworthiness of the nodes in the network and the QoS of the proposed secure QoS routing protocol in both security and performance. It's also to be extent using the cryptographic technique called Elliptic Curve Cryptography and also to perform secure data transfer using Adhoc networks.

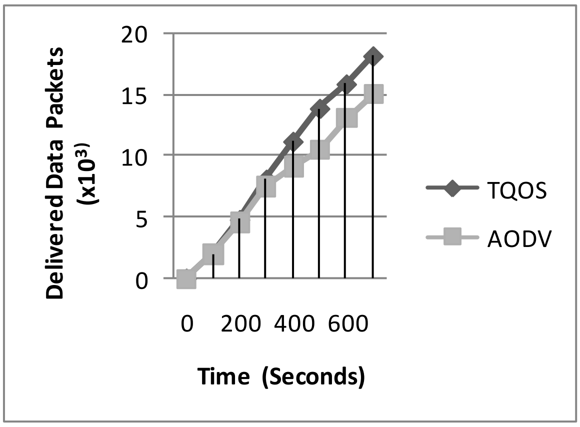

Fig. 2. The total number of packet delivered in the presence of 5 malicious nodes in a network with 50 nodes

The graph shown in Fig.2 is to mention the trust worthiness and the secure routing protocol as it determined. By looking at it the trustworthiness doesn't took much part in the previous.

For these reasons, to propose a new secure routing protocol. First, it is able to detect the difficult internal attacks, including Byzantine attacks by identifying the malicious node. Second, the results on the message verification conducted by a node are used to build a trustworthiness repository by the node on its neighbouring nodes that deliver the message. Third, the trustworthiness is incorporated into the routing metrics, which contains the QoS requirement on the links along a route, such as packet delay and link quality. Secure Route Discovery, Secure Route Setup and maintenance are kept as an integral part of the project.

Thus the scope of the project depends upon the finding the malicious node and its durability in the time. Such that in includes cryptographic technique to transfer data in secure manner.

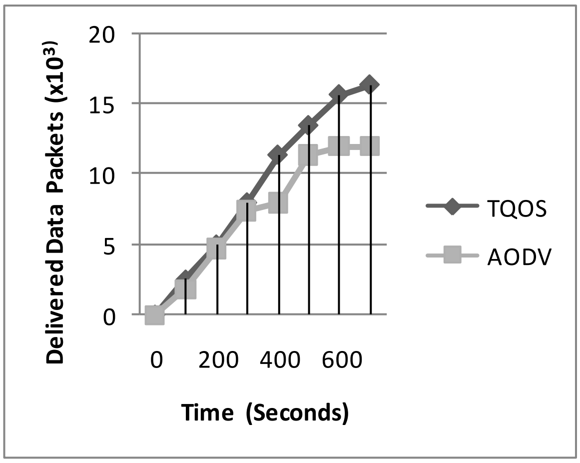

Fig. 3. The total number of packet delivered in the presence of 10 malicious nodes in a network with 50 nodes

As the Fig.3 describes the protocol work implementing in the session, as such it has been demonstrated in simulated with the help of network simulator tool it brings change in the outcome

3.1 AN ELLIPITIC CURVE CRYPTOGRAPHY

Asymmetric cryptography is a marvelous technology. Its uses are many and varied. And when you need it, you need it. For many situations in distributed network An environment, asymmetric cryptography is a must during communications. If you're taming key distribution issues with a public key infrastructure (PKI), you're using asymmetric cryptography. If you're designing or employing any kind of network protocol or application requiring secure communications, to come up with a practical solution, you're going to have to use asymmetric cryptography. Asymmetric cryptography has, in fact, proved so useful for securing Communications that it has become pervasive in modern life. Every time you buy something on the Internet, if the vendor is using a secure server, you're using asymmetric cryptography to secure the transaction. But asymmetric cryptography is demanding and complex, by its very nature. The hard problems in number theory the key to the algorithms' functionality are all intrinsically difficult enough that the processor cycles you must throw at doing it, and/or the chip space you must dedicate to the implementation, inevitably far outstrip the resources you must dedicate for doing symmetric cryptography.

3.1 DISTRIBUTION KEY ESTABLISHMENT

The key setup can also be done in a distributed way. In the distributed key establishment, each L-sensor is pre-loaded with a pair of ECC keys - a private key and a public key. When an L-sensor (denoted as *u*) sends its locations information to its cluster head H, *u* computes a Message Authentication Code (MAC) over the message by using *u*'s private key, and the MAC is appended to message. When H receives the message, H can verify the MAC and then authenticate *u*'s identify, by using *u*'s public key. Then H generates a certificate (denoted as CA*u*) for *u*'s public key by using H's private key. After determining the routing tree structure in a cluster, the cluster head H disseminates the tree structure (i.e., parent child relationship) and the corresponding public key certificate to each L-sensor. The public key certificates are signed by H's private key, and can be verified by every L-sensor, since each L-sensor is preloaded with H's public key. A public key certificate proves the authenticity of a public key and further proves the identity of one L-sensor to another L-sensor. For example, suppose that L-sensor *u* and *v* are *c*neighbors and *u* has a smaller ID than *v*. The process is presented below:

1) Node u sends its public key KU u = IuP to v.
2) Node v sends its public key KU v = IvP to u.
3) Node u generates the shared key by multiplying its Private key *Iu* with *v*'s public key – *KU v* , i.e., *Ku,v* = *KR u KUv* = *IuIvP*; similarly, *v* generates the shared key - *Ku,v* = *KR v KU u* = *IuIvP*.

After the above process, nodes *u* and *v* share a common Key and they can start secure communications. To reduce the computation overhead, symmetric encryption algorithms are used among L-sensors. Note that in the distributed key establishment scheme, the assumption of having tamper-resistant hardware in H-sensors can be removed.

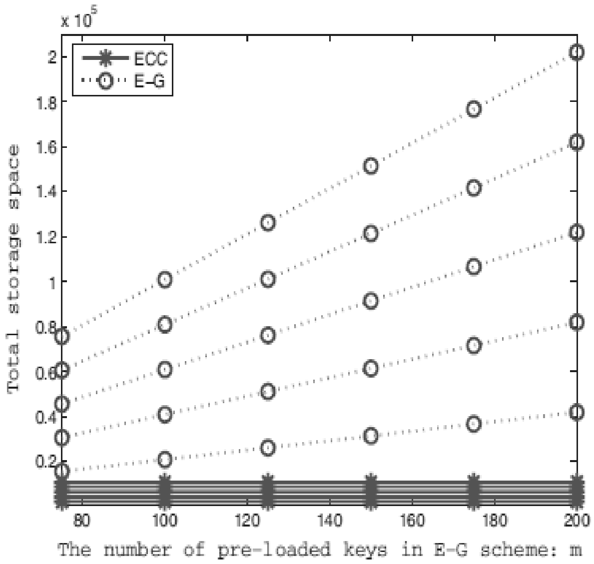

Fig. 4.Comparision of required storage space

In Fig. 4, plot the total storage requirements for different sizes of sensor networks and different numbers of pre-loaded keys in the E-G scheme. The *x*-axis is *m* - the number of pre-loaded keys in the E-G scheme. The *y*-axis represents the total storage space required for pre-loaded keys (in the unit of key length). The top five dotted curves (with small circles) are the total required storage spaces under the E-G scheme, where *N* = 1,000, 800, 600, 400, and 200 from top to bottom respectively. The five solid lines at the bottom of Fig. 4 are the total required memory spaces under

the centralized ECC key management scheme, for the five value of *N* (1,000, 800, 600, 400, and 200). Fig. 2 shows that the ECC key management scheme requires much less storage space for pre-loaded keys than the E-G scheme, for different network sizes and numbers of pre-loaded keys (*m*) tested. The more keys pre-loaded in a sensor under the E-G scheme, the larger the storage saving achieved by the ECC scheme.

4.0 CONCLUSION

In this paper, this address the most challenging problem of designing a secure routing protocol with QoS support. For a routing protocol to detect the major internal attacks such as Byzantine attacks, to propose to use both route and message redundancies during topology discovery. The attacks can be detected by verifying various copies of a received message, which reaches a node via different path, sat different times. By combining the security mechanism with QoS requirements, to present a secure QoS routing protocol
That achieves better performance than the existing ones, as demonstrated by simulation results. It is worth pointing out that the message redundancy is enforced by sending a same message a few times if the route
Redundancy does not exist. Also, it is assumed that the source and its intended destination are trusted, which are established by an external trust agent or CA.
The Future work going to be done is that the message has to be sending in secured means of transfer through the cryptography technique such the integrity would not affect. Connection establishment done by TCP and the nodes authenticate for the secure transfer.

REFERENCES

[1] R. Perlman, “Routing with Byzantine robustness," report no: TR-2005-146 [Online] Available: http: //research.sun.com/ techrep / 2005/smli_tr-2005-146.pdf, Sept. 2005.

[2] D. Bertsekas and R. Gallary, *Data Networks*, 2nd ed., Section 5.6 and 5.7. Prentice-Hall, 1992.

[3] Zhang, M. C. Zhou, and M. Yu, “Ad hoc network security: a review," Int. J. Commun. Syst., vol. 20, no. 8, pp. 909-925, Aug. 2007.

[4] U. Kremer, J. Hicks, and J. M. Rehg, “A compilation frameworkfor power and energy management on mobile computers," Dept. CS Technical Report, DCS-TR-446, Rutgers University, June 2001.

[5] S. Capkun, L. Buttyan, and J. Hubaux, “Self-organized public-key management for mobile ad hoc networks," *IEEE Trans. Mobile computing*, vol. 2, no. 1, pp. 1-13, Jan./Mar. 2003.

[6] M. Yu, A. Malvankar, and W. Su, “A distributed radio channel allocation scheme for WLANs with multiple data rates," IEEE Trans. Commun., vol.56, no. 3, Mar. 2008.

[7] S. Capkun, L. Buttyan, and J. Hubaux, “Self-organized public-key management for mobile ad hoc networks," *IEEE Trans. Mobile Computing*, vol. 2, no. 1, pp. 1-13, Jan./Mar. 2003.

[8] J. Dowling, E. Curran, R. Cunningham, and V. Cahil, “Using feedback in collaborative reinforcement learning to adaptively optimize MANET routing," *IEEE Trans. SMC, Part A: Systems Humans*, pp. 360-372, vol.35, no. 3, May 2005.

[9] B. Awerbuch, R. Curtmola, D. Holmer, and C. Nita-Rotaru, “ODSBR: an on-demand secure Byzantine routing protocol," JHU CS Technical Report v.1, Oct. 15th, 2003.

[10] D. Boneh, C. Gentry, H. Shacham, and B. Lynn, “Aggregate and verifiably encrypted signatures from bilinear maps," in *Proc. Advances in Cryptology - Eurocrypt03*, LNCS, 2003.

[11] W. Liu, W. Lou, and Y. Fang, “An efficient quality of service routing algorithm for delay-sensitive applications," Computer Networks, vol. 47, no. 1, pp. 87-104, 2005.

[12] L. Eschenauer and V. D. Gligor, “A key management scheme for distributed sensor networks,” in *Proc. 9th ACM Conference on Computerand Communication Security*, pp. 41-47, Nov. 2002.

Author Profile:

S. Ravichandran – **S. Ravichandran** is an Associate Professor in Department of Information Technology at Sri Krishna Engineering College.

He received the Master of Computer Applications in Bharathidhasan University at 1996, he received the Master of Philosophy in Computer Science in Madurai Kamaraj University at 2007, he received the Master of Engineering in Computer Science and Engineering from Anna University at 2010 and now he is perusing Doctorate of Philosophy in Computer Science at Bharathiar University. He has 17 Years of teaching experiences from various Engineering Colleges. He has published two papers in International journals and he has presented in 13 International Conferences & presentd in 16 National Conferences in various Engineering Colleges. His area of interest includes Cloud Computing, Artificial Intelligence, Networks and Compilers.